Structured Information Security Risk Management for Operational Risk Mitigation in Standard Chartered Bank: A Case Study

Carsten Paasch
CISO
SC First Bank, Korea

AGENDA

1. Brief Facts on Standard Chartered Bank
2. Information Security and Operational Risk Management
3. Information Security Risk Management
   A. The Risk Model
   B. The Risk Analysis Process
   C. The Tool
4. Conclusion

SCB: Some Facts

- UK-based Banking Group
  - Consumer Banking (Private Customers, SME)
  - Wholesale Banking (Corporate Banking, Global Markets)
- Active in nearly 60 Countries
- Global Staff Size About 45,000
- Major Markets
  - Korea (7000+ Staff, 400+ branches)
  - Hong Kong (4000+ staff, 70+ Branches)
  - Singapore (2500+ staff, 20+ Branches)
  - India (8000+ staff, 80+ Branches)

SCB: Some Facts

US$m	2004	2005	YoY%
Income	5,382	6,861	27
Expenses	(2,849)	(3,811)	34
Operating profit before provisions	2,533	3,050	20
Loan impairment	(214)	(319)	49
Other impairment	(68)	(50)	(26)
Profit before tax	2,251	2,681	19

Information Security at SCB

- Part of Technology and Operations
- Independent from Production IT and IT Development
- Staff in Singapore, UK, Malaysia, India, and Korea
- 4 Core Teams
  - Operational IT Security
  - Policy and Risk (5 risk managers globally) → small team!
  - Engineering and Architecture
  - Communications and Awareness
- 2 Special Teams
  - Innovation Lab
  - Information Security at SC First Bank Korea

AGENDA

1. Brief Facts on Standard Chartered Bank
2. Information Security and Operational Risk Management
3. Information Security Risk Management
   A. The Risk Model
   B. The Risk Analysis Process
   C. The Tool
4. Conclusion

Operational Risk

- Basel II definition: The risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events.
- Three approaches:
  - Basic Indicator Approach
  - Standardized Approach
  - Advanced Measurement Approach

OR and Information Security

- ***Information is critical to the operation of every financial institution.***
  - If the confidentiality of sensitive or private information is compromised, lawsuits or regulatory sanctions may result in penalties, and violated trust may result in customer flight.
  - If the integrity of critical information is corrupted, errors in processing may occur with similar negative consequences.
  - If critical information is not available where and when it is needed, important processes may fail completely with similar results.
- **Information security controls are among the foundation stones of operational risk management.**
- **Information security risks are part of the bank's overall operational risk landscape**
- **→Information Security risk needs to be managed being a part of operational risk management**

Information Security Risk Management

- Too little information security will result in too much information security risk and consequentially operational risk
- Too much information security is expensive and counter-productive to the business
- A balance needs to be struck
- A structured risk assessment and management method for information security risk is needed
  - To define appropriate security for systems in line with the desired risk profile
  - Neither over-protecting nor under-protecting
- BUT HOW TO DO THAT….?

"Risk Assessment" in the context of information security

DEFINITION as per BS7799:

Risk Assessment is the systematic consideration of

a) **Business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;**

b) **The realistic likelihood of such failure occurring in the light of prevailing threats and vulnerabilities and the controls currently implemented.**

- → Risk = Business Harm x Likelihood

What are the overriding objectives in Information Security Risk Management?

1. Ensure the right level of security is achieved in every case, in line with policies and standards.

2. Ensure consistency across countries and business lines while being able to cater for variations in risk appetite and threat environment.

3. Ensure the Information Security department is not a bottleneck in the process despite small size.

4. Ensure that any tools used in risk analysis process are easily accessible, easy to understand and easy to use.

How to apply this in practice?

1. Develop a RISK MODEL that implements the idea of defining RISK= IMPACT x LIKELIHOOD in the context of
    1. Confidentiality
    2. Integrity
    3. Availability

2. Develop a structured risk analysis PROCESS to apply this model to
    1. New system developments
    2. Systems in production

3. Implement TOOLS to facilitate and accelerate the process and remove bottlenecks

AGENDA

1. Brief Facts on Standard Chartered Bank
2. Information Security and Operational Risk Management
3. Information Security Risk Management
   A. The Risk Model
   B. The Risk Analysis Process
   C. The Tool
4. Conclusion

Setting the Scene - Definitions

Standard Chartered

1. Threat

- **Scenario where a Vulnerability is exploited with potentially undesirable Impact on the business**
- **Examples:**
  - ⇨ Natural disaster
  - ⇨ Hacker attacks
- **Each Threat has an Inherent Likelihood**

2. Control

- **A policy, method, procedure, device or programmed mechanism which reduces the Likelihood (and/or Impact) of a specific Threat**

3. Vulnerability

- **Weakness or flaw in a system which has the potential to be exploited by a threat and to result in a damaging Impact**
  - ⇨ ie. when a Control is absent

Definitions (2)

4. Asset

- **Item, or class of information items owned by business**
- **Has an intrinsic value to the business**
- **Value measured with regards to**
  - ⇨ Confidentiality (what is the secrecy of information worth)
  - ⇨ Integrity (what is the integrity of information worth)
  - ⇨ Availability (what is it worth that information is available)

5. Impact

- **Unwanted or adverse effect that a Threat would have on the business**
- **The inverse of "Value"**

Definitions (3): RISK

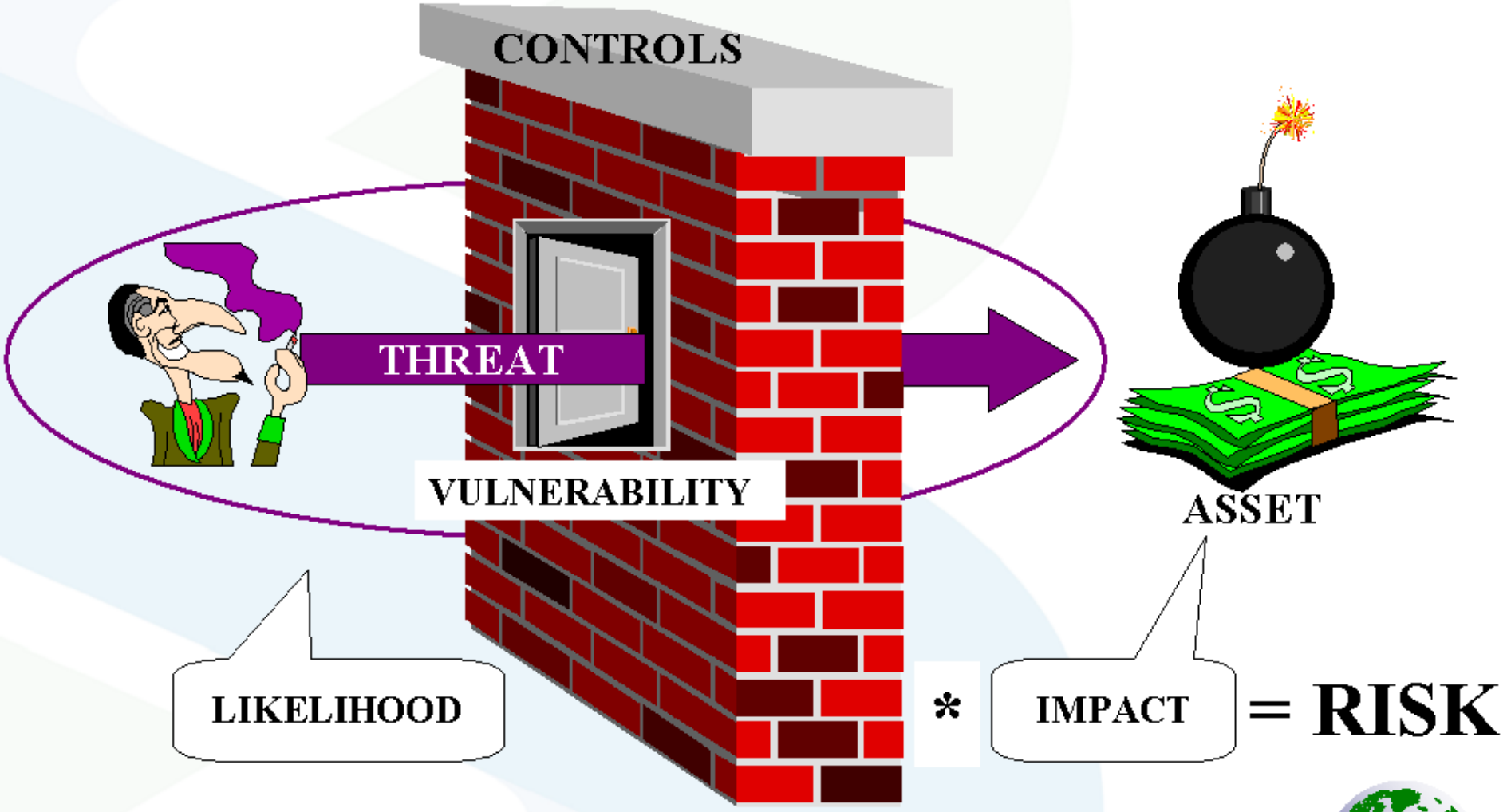
- In single Threat-Impact Scenario:
  RISK = LIKELIHOOD x IMPACT

- In multiple Threat-Impact Scenarios:
  - TOTAL RISK is the aggregate (for each Asset and each Threat) of the single threat-impact scenario values:

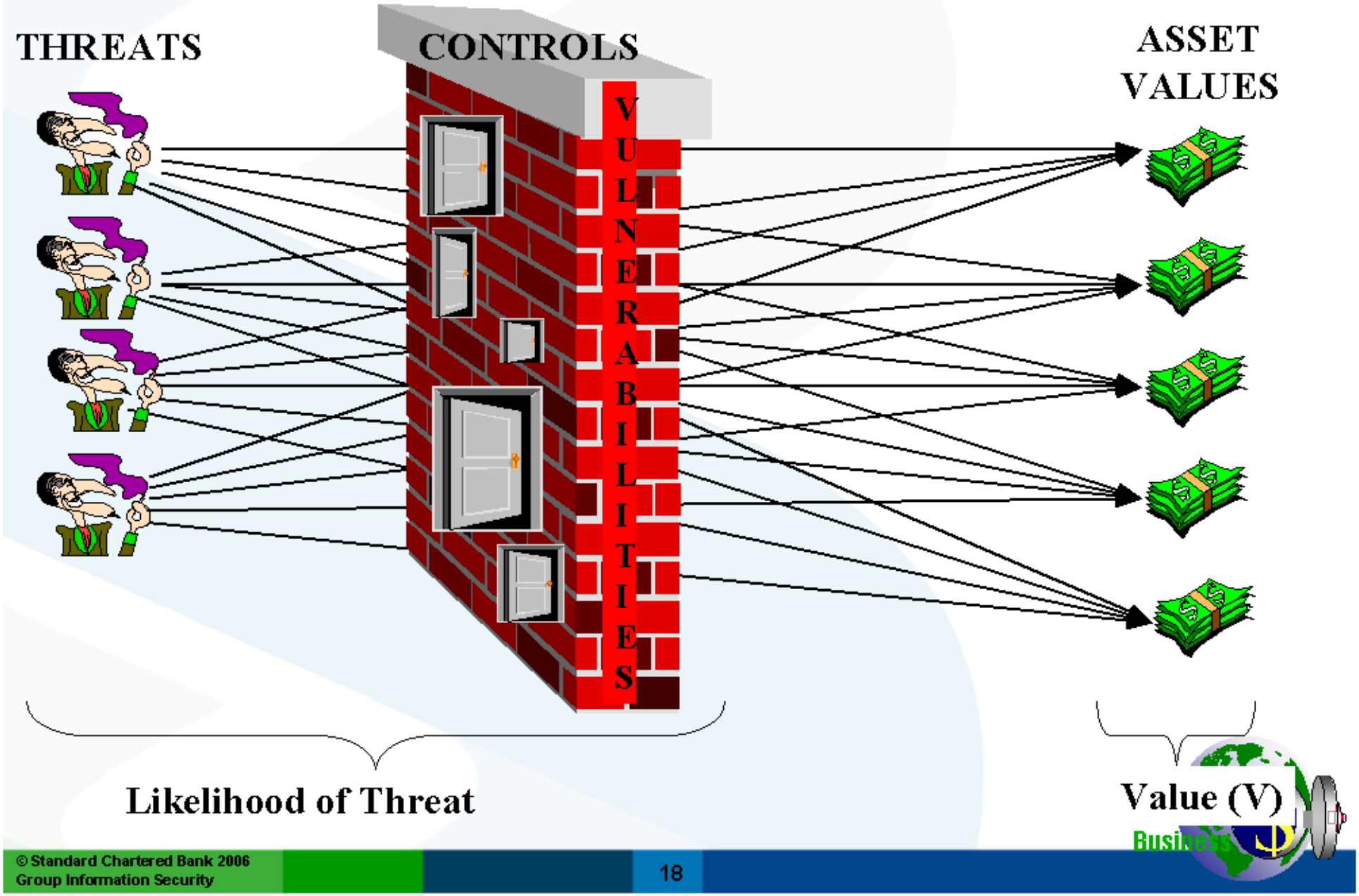
TOTAL RISK= $\sum^{A} \sum^{Th}$ **Likelihood (Threat) * Impact of Threat**

Total Target Risk should become LOW through the choice of appropriately chosen Controls.

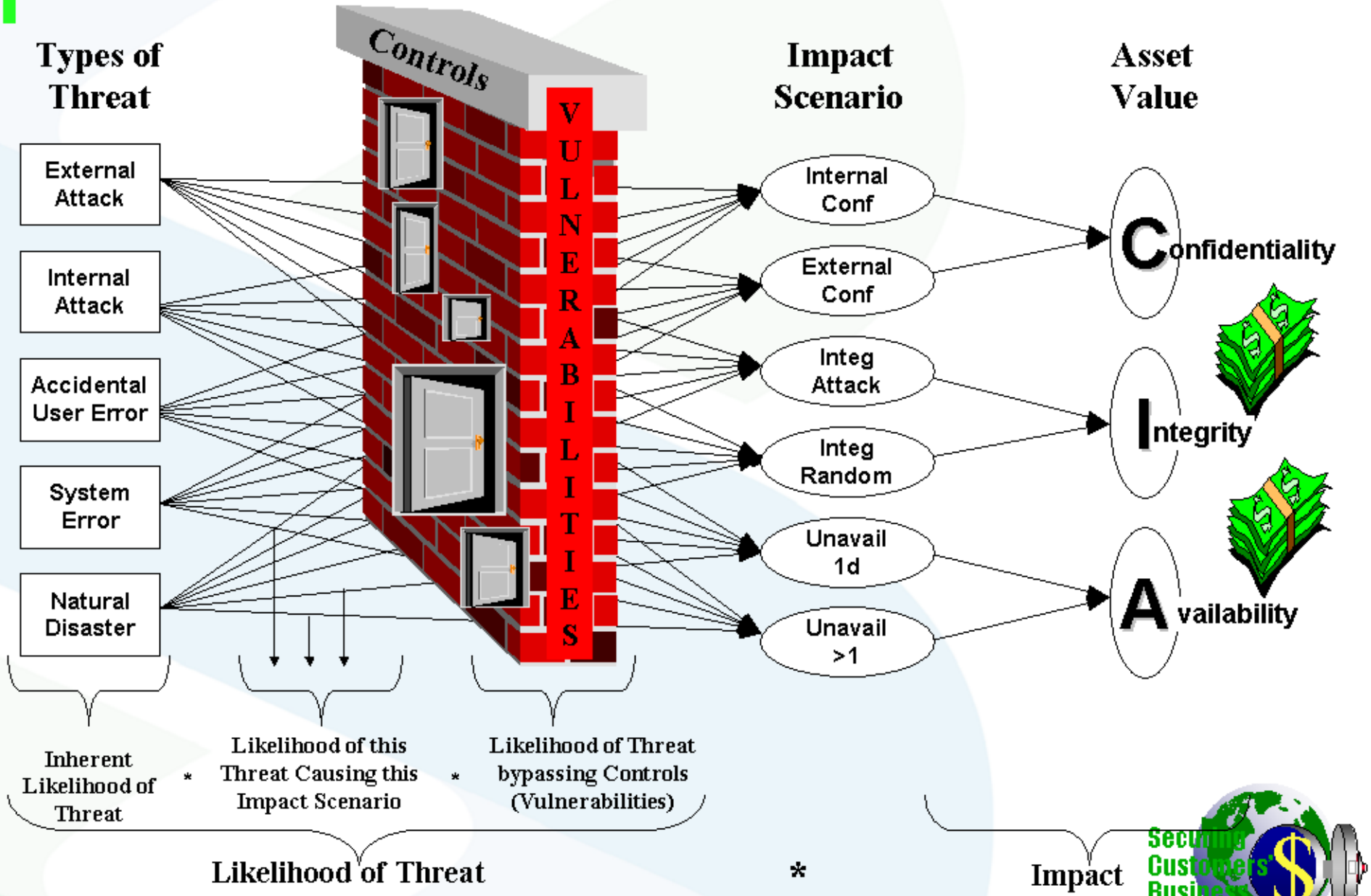
Single Threat/Vulnerability Scenario



Multiple Threat/Vulnerability Scenario



Standard Chartered Risk Model



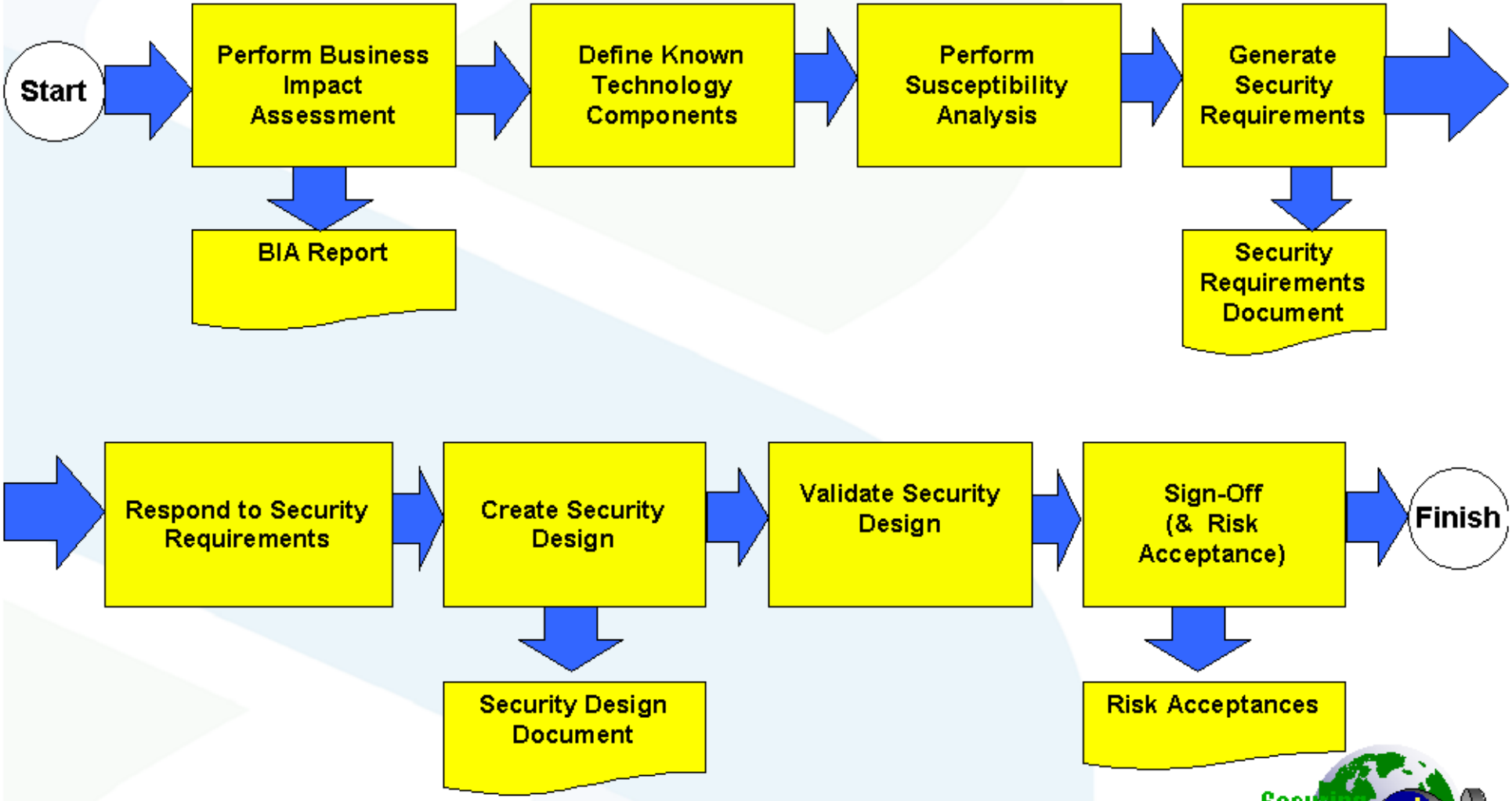
AGENDA

1. Brief Facts on Standard Chartered Bank
2. Information Security and Operational Risk Management
3. Information Security Risk Management
   A. The Risk Model
   B. The Risk Analysis Process
   C. The Tool
4. Conclusion

Objectives of Risk Analysis Process

- Define security requirements during system design
- Identify *appropriate* Security Requirements based on:
  - Business Impact Assessment (BIA) and Susceptibility Analysis (Applying the Risk Model)
  - Technology and architecture of the system
- Record compliance with Security Requirements
- Record areas of non-compliance as risks
  - Threat/Vulnerability assessment based on BIA
  - Formal risk acceptance
- Make process transparent to all stakeholders
- Integrate with IT development lifecycle
- Devolve Risk Process to project teams

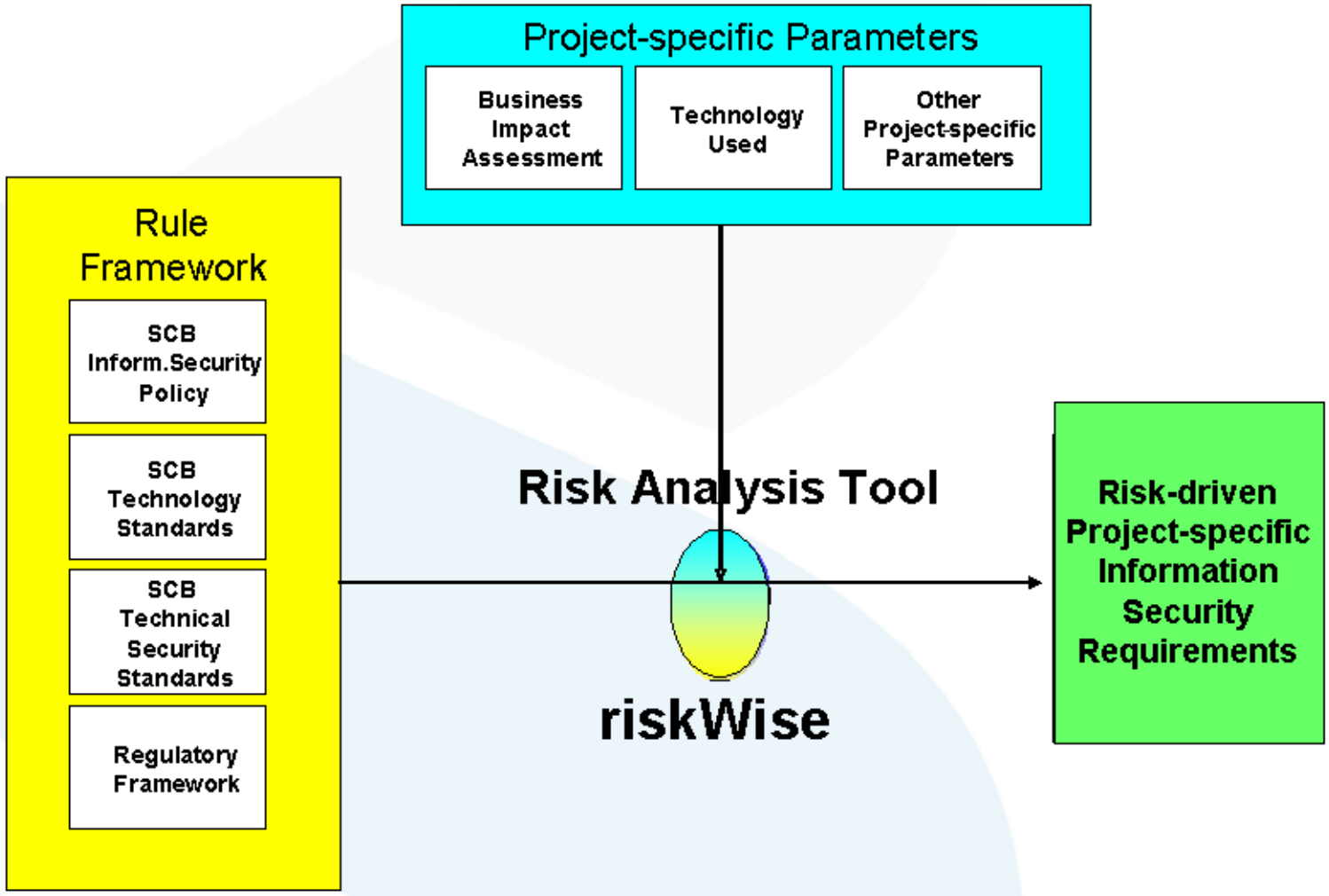
Risk Analysis during system design



AGENDA

1. Brief Facts on Standard Chartered Bank
2. Information Security and Operational Risk Management
3. Information Security Risk Management
   A. The Risk Model
   B. The Risk Analysis Process
   C. The Tool
4. Conclusion

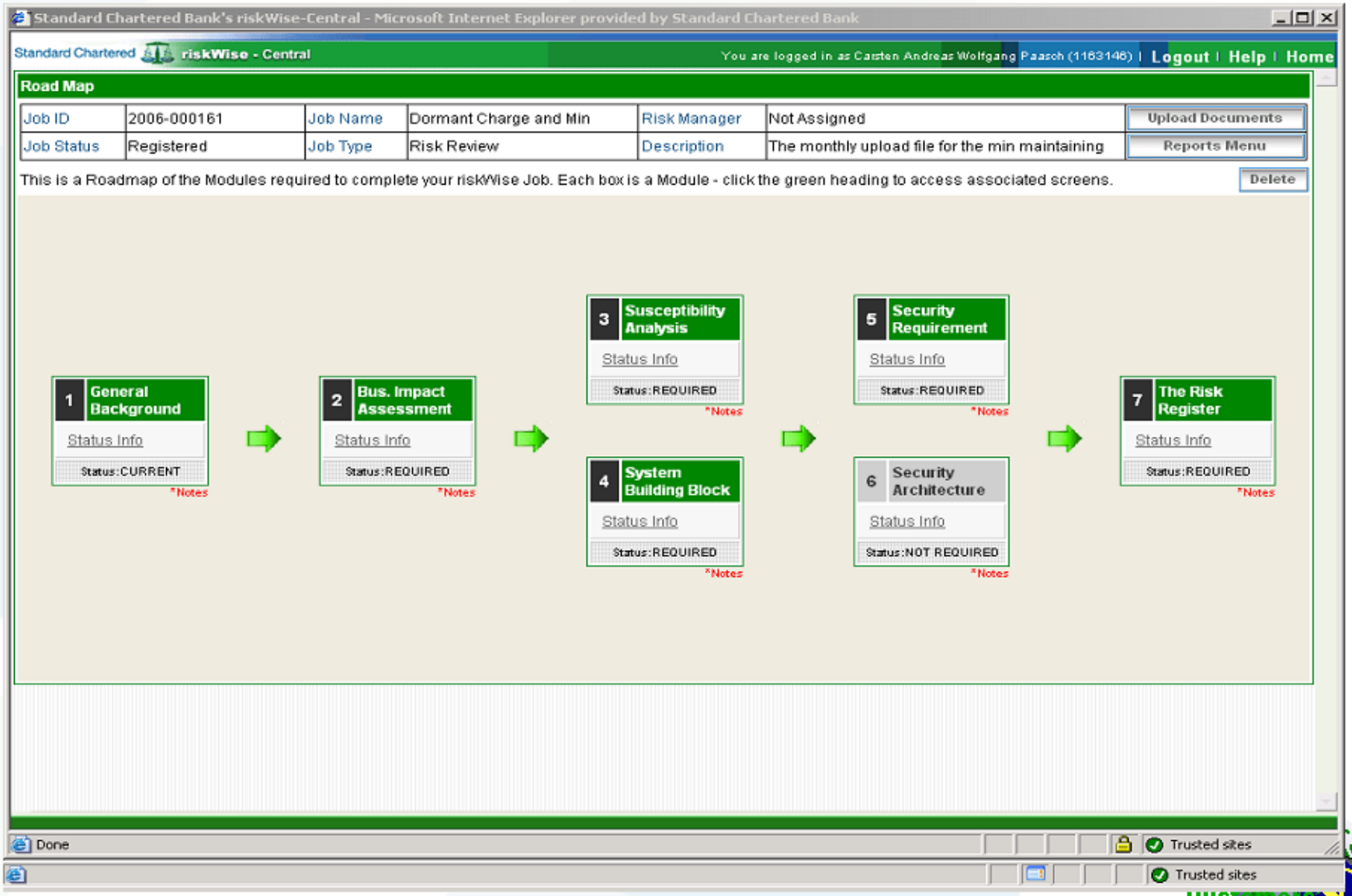
Conceptual Approach



SCB Risk Analysis Tool: riskWise

- Tool accessible from anywhere on SCB Intranet
- Browser-based
- Implements the risk model
- Filters based on technology building block information
- Supports the risk analysis process
- Used as information security risk register
- Won “Best Security Implementation” Award by Secure Computing Magazine in April 2005

riskWise - Screenshot



Conclusion

- Information security risk management is a crucial component of operational risk management
- Information security risk analysis is meant to determine the right level of security to protect the bank's information assets
- This requires a good
  - Risk Model
  - Risk Analysis Process
  - A Tool to support the above
- We like to think we have achieved it…

Questions?

For further information, please contact:

Carsten.Paasch@hk.standardchartered.com

+82 2 3433 2858

+82 10 4820 0232